WE CLAIM:

1. A secure disk drive comprising:

(a) a disk for storing data;

(b) an input for receiving an encrypted message from a client disk drive, the encrypted message comprising ciphertext data and a client drive ID identifying the client disk drive;

(c) a secure drive key;

(d) an internal drive ID;

(e) a key generator for generating a client drive key based on the client drive ID and the secure drive key, and an internal drive key based on the internal drive ID and the secure drive key;

(f) an authenticator for verifying the authenticity of the encrypted message and generating an enable signal, the authenticator responsive to the encrypted message and the client drive key;

(g) a data processor comprising:

a message input for receiving the encrypted message from the client disk drive;

a data output for outputting the ciphertext data to be written to the disk;

an enable input for receiving the enable signal for enabling the data processor;

a key input for receiving the internal drive key, the internal drive key for use in generating a message authentication code; and

a reply output for outputting reply data, the reply data comprising the message authentication code; and

(h) an output for outputting a reply to the client disk drive, the reply comprising the reply data and the internal drive ID.

2. The secure disk drive of claim 1, wherein the secure drive key is immutable.

3. The secure disk drive of claim 1, wherein the secure drive key is mutable.

4. The secure disk drive of claim 1, wherein the authenticator comprises a means for verifying the access rights of the client drive ID.

5. The secure disk drive of claim 1, wherein the secure drive key comprises tamper resistant circuitry.

6. The secure disk drive of claim 1, wherein the key generator comprises tamper resistant circuitry.

7. The secure disk drive as recited in claim 1, wherein the authenticator comprises tamper resistant circuitry.

8. The secure disk drive as recited in claim 1, wherein the data processor further comprises cryptographic facilities.

9. A secure disk drive comprising:

(a) a disk for storing data;

(b) an input for receiving an encrypted message from a client disk drive, the encrypted message comprising ciphertext data and a client drive ID identifying the client disk drive;

(c) a secure drive key;

(d) an internal drive ID;

(e) a key generator for generating a client drive key based on the client drive ID and the secure drive key, and an internal drive key based on the internal drive ID and the secure drive key;

(f) an authenticator for verifying the authenticity of the encrypted message and generating an enable signal, the authenticator responsive to the encrypted message and the client drive key;

(g) a data processor comprising:

a message input for receiving the encrypted message from the client secure disk drive;

a data input for receiving ciphertext data read from the disk;

an enable input for receiving the enable signal for enabling the data processor;

a key input for receiving the internal drive key, the internal drive key for use in generating a message authentication code; and

a reply output for outputting reply data, the reply data comprising the ciphertext data read from the disk and the message authentication code; and

(h) an output for outputting a reply to the client disk drive, the reply comprising the reply data and the internal drive ID.

10. The secure disk drive of claim 9, wherein the secure drive key is immutable.

11. The secure disk drive of claim 9, wherein the secure drive key is mutable.

12. The secure disk drive of claim 9, wherein the authenticator comprises a means for verifying the access rights of the client drive ID.

13. The secure disk drive of claim 9, wherein the secure drive key comprises tamper resistant circuitry.

14. The secure disk drive of claim 9, wherein the key generator comprises tamper resistant circuitry.

15. The secure disk drive as recited in claim 9, wherein the authenticator comprises tamper resistant circuitry.

16. The secure disk drive as recited in claim 9, wherein the data processor further comprises cryptographic facilities.